XKEYSCORE Workflows

19 September 2011

DERIVED FROM: NSA/CSSM 1-52
DATED: 20070108
DECLASSIFY ON: 20320108

What is a workflow?

- Workflows automate queries.
  - One-time
  - Standing
- Every search type can be a workflow.
  - Same functionality and capability
- Follow on actions
  - Email alert
  - Download actions
  - Metadata summary

Who can submit a workflow?

- Anyone!
- One owner per workflow, but using follow-on actions:
  - Multiple-users can be notified of results and/or sent summary information
  - Result table can be automatically shared
- If ownership needs to be changed, a ticket can be submitted to the team.

What can I do with a workflow?

- Workflows can be configured to run once
- Workflows can be configured to run daily
  - Every 1, 2, 3, 4, 6, 8, 12 or 24 hours
  - You can set an offset to start running at a certain hour
- Download results
- Email results and email alerts
- MAILORDER results
- MySQL report

Why do I want a workflow?

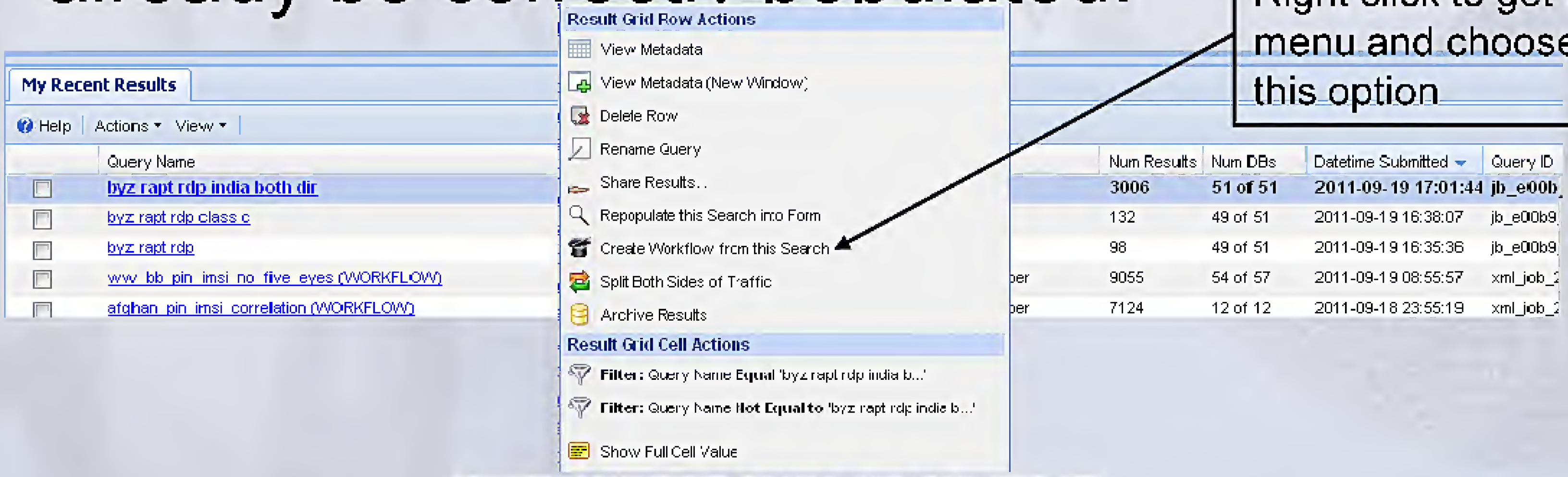
- XKEYSCORE has a rolling buffer of data
- Repetitive queries
- Sigdev purpose
  - Fingerprint and appid testing
- Queries take a long time during high times
- Follow on actions
  - Google Earth data
  - Statistics
  - Customizable – write a script!

How do I setup a workflow?

- Two main ways
  - Based on the results of a recent query
    - Simplifies the process & more likely to produce the desired result!
    - This is done by right-clicking on the result set from the desired query and selecting *Create Workflow from this Search*. This populates the Workflow Wizard with the same criteria that was used by the selected query.
  - From scratch using the Workflow Wizard
    - Not recommended – but we'll show you anyway

How do I setup a workflow?

- The next ten slides demonstrate how to step through the workflow wizard from scratch
- But if you create the workflow from an existing query result many of the steps will already be correctly populated!



My Recent Results

Help | Actions ▾ | View ▾

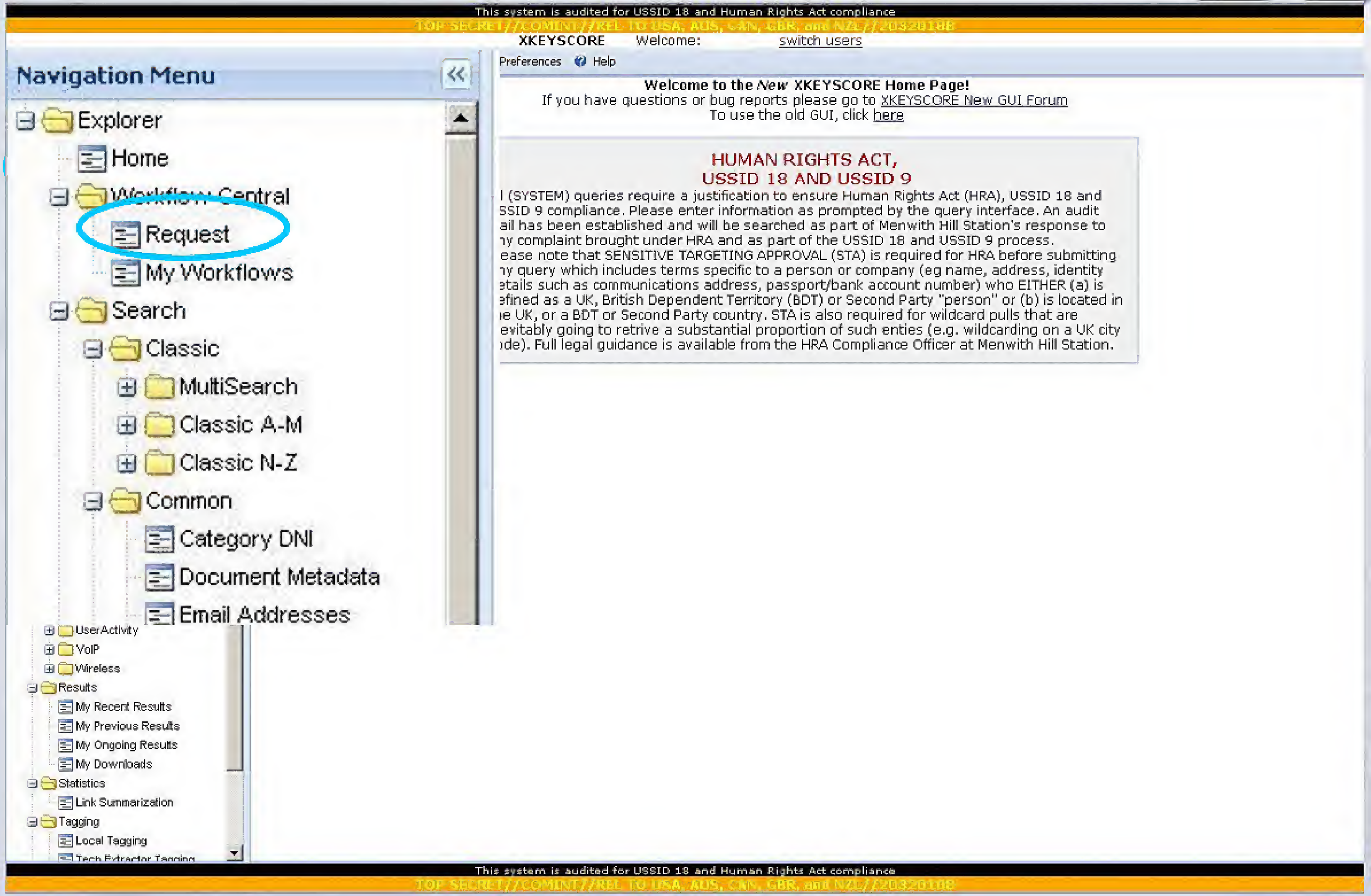
	Query Name		Num Results	Num DBs	Datetime Submitted	Query ID
□	byz rapt rdp india both dir		3006	51 of 51	2011-09-19 17:01:44	jb_e00b
□	byz rapt rdp class c		132	49 of 51	2011-09-19 16:38:07	jb_e00b9
□	byz rapt rdp		98	49 of 51	2011-09-19 16:35:36	jb_e00b9
□	ww_bb_pin_imsi_no_five_eyes (WORKFLOW)	ber	9055	54 of 57	2011-09-19 08:55:57	xml_job_2
□	afghan_pin_imsi_correlation (WORKFLOW)	ber	7124	12 of 12	2011-09-18 23:55:19	xml_job_2

Result Grid Row Actions
- View Metadata
- View Metadata (New Window)
- Delete Row
- Rename Query
- Share Results...
- Repopulate this Search into Form
- Create Workflow from this Search
- Split Both Sides of Traffic
- Archive Results

Result Grid Cell Actions
- **Filter:** Query Name **Equal** 'byz rapt rdp india b...'
- **Filter:** Query Name **Not Equal to** 'byz rapt rdp india b...'
- Show Full Cell Value

Right click to get the menu and choose this option

How do I setup a workflow?



This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

Welcome to the *New* XKEYSCORE Home Page!
If you have questions or bug reports please go to XKEYSCORE New GUI Forum
To use the old GUI, click here

HUMAN RIGHTS ACT,
USSID 18 AND USSID 9

l (SYSTEM) queries require a justification to ensure Human Rights Act (HRA), USSID 18 and SSID 9 compliance. Please enter information as prompted by the query interface. An audit ail has been established and will be searched as part of Menwith Hill Station's response to ny complaint brought under HRA and as part of the USSID 18 and USSID 9 process. ease note that SENSITIVE TARGETING APPROVAL (STA) is required for HRA before submitting ny query which includes terms specific to a person or company (eg name, address, identity etails such as communications address, passport/bank account number) who EITHER (a) is efined as a UK, British Dependent Territory (BDT) or Second Party "person" or (b) is located in ie UK, or a BDT or Second Party country. STA is also required for wildcard pulls that are evitably going to retrive a substantial proportion of such enties (e.g. wildcarding on a UK city ode). Full legal guidance is available from the HRA Compliance Officer at Menwith Hill Station.

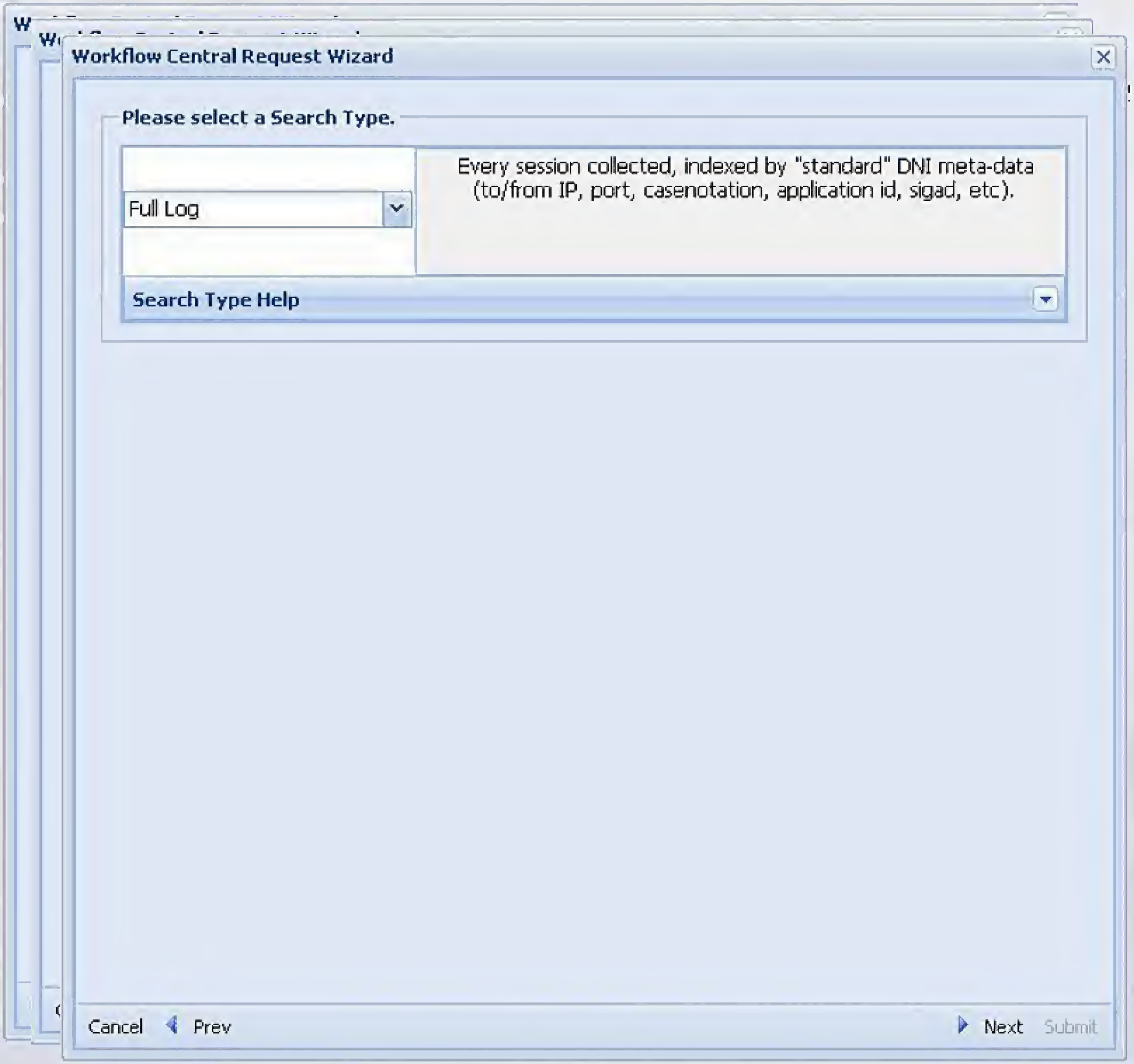
This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

How do I setup a workflow?

First, s a

workflc



Workflow Central Request Wizard

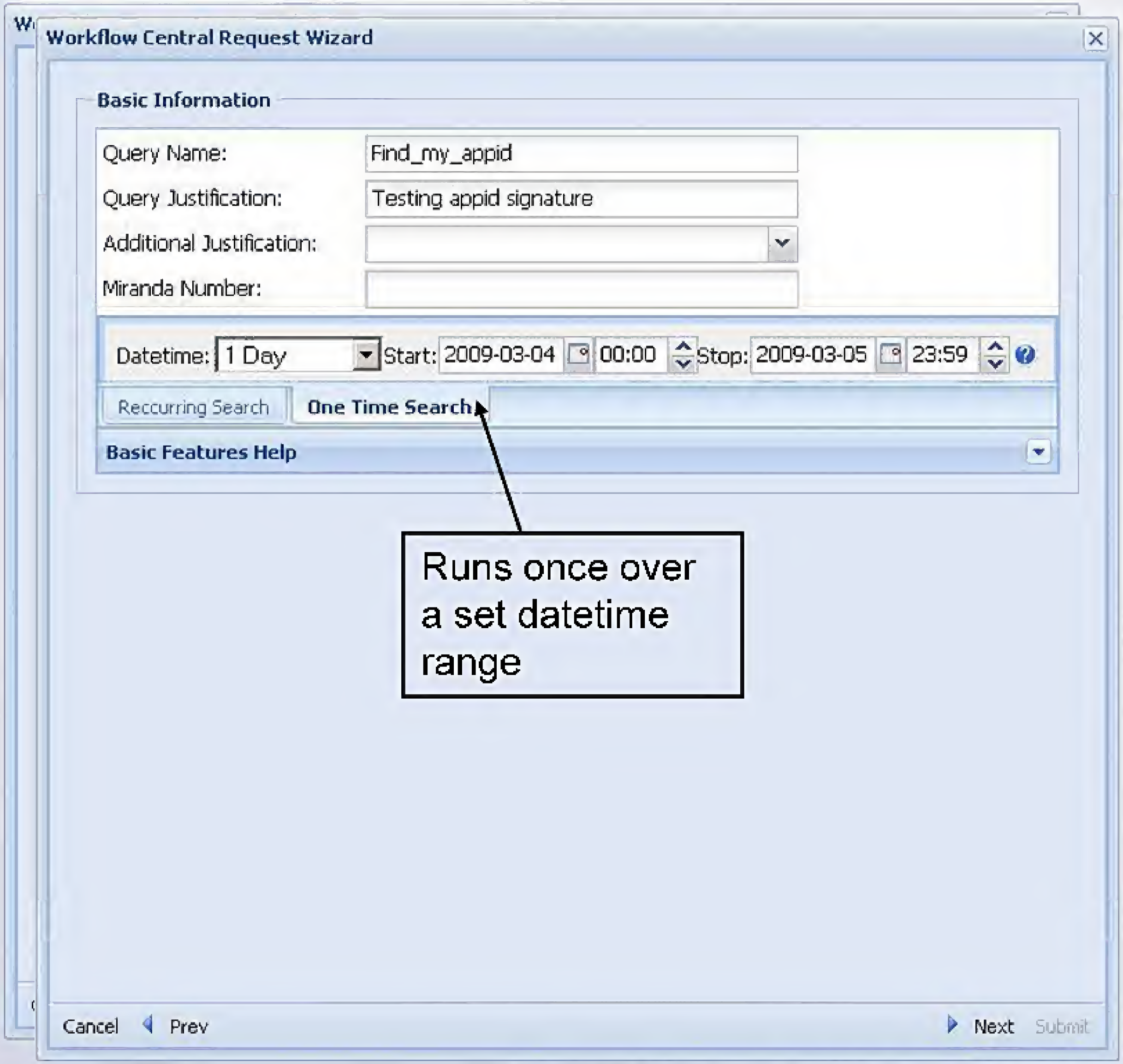
Please select a Search Type.

Full Log

Every session collected, indexed by "standard" DNI meta-data (to/from IP, port, casenotation, application id, sigad, etc).

Search Type Help

How do I setup a workflow?



Workflow Central Request Wizard

Basic Information

Query Name:	Find_my_appid
Query Justification:	Testing appid signature
Additional Justification:	
Miranda Number:	

Datetime: 1 Day Start: 2009-03-04 00:00 Stop: 2009-03-05 23:59

Runs once over a set datetime range

ring or one-

ıst be unique per user

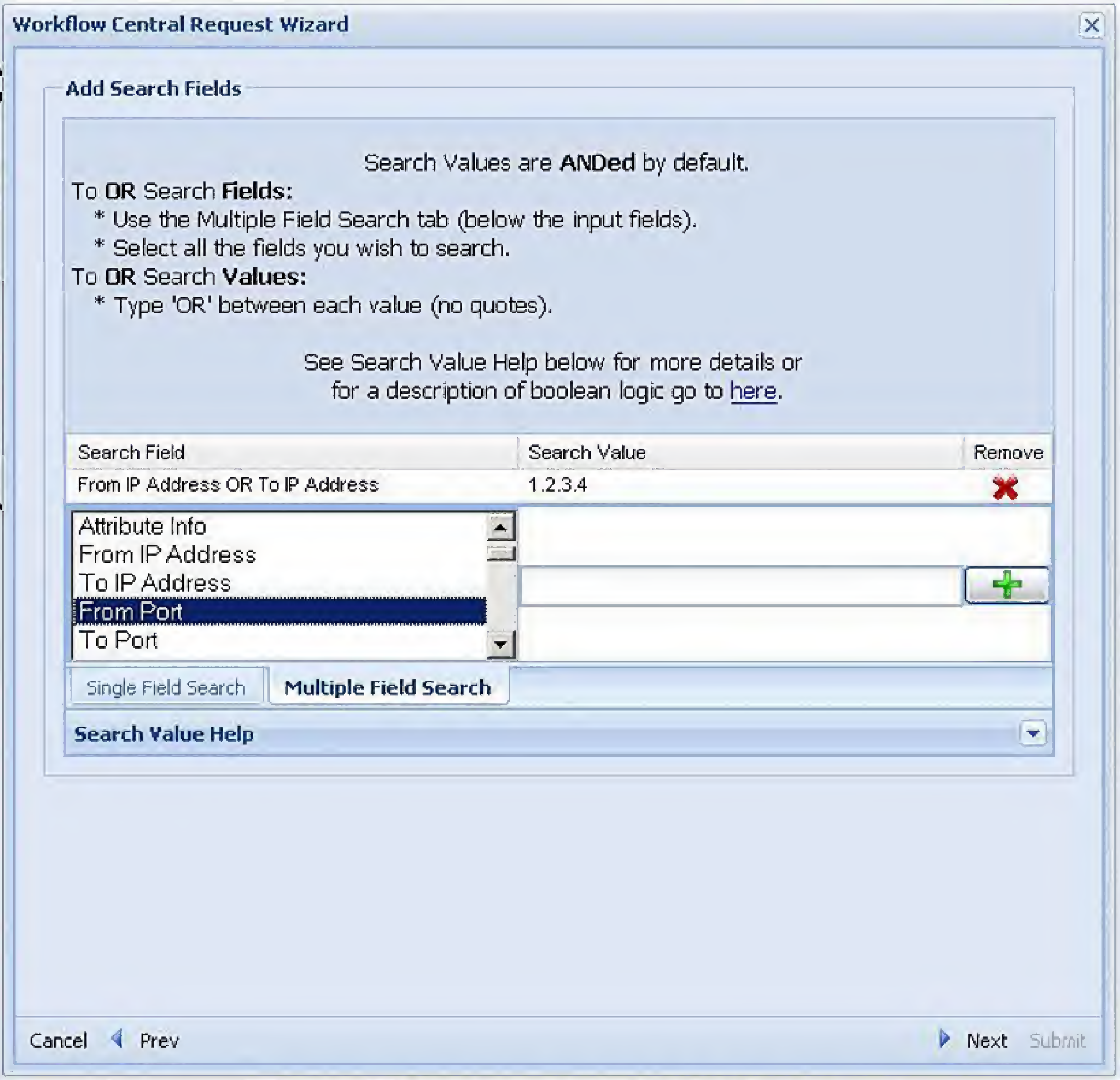
must have a justification

justifications

How do I setup a workflow?

Selec ant to searc

Select a field to search



Workflow Central Request Wizard

Add Search Fields

Search Values are ANDed by default.
To OR Search Fields:
* Use the Multiple Field Search tab (below the input fields).
* Select all the fields you wish to search.
To OR Search Values:
* Type 'OR' between each value (no quotes).

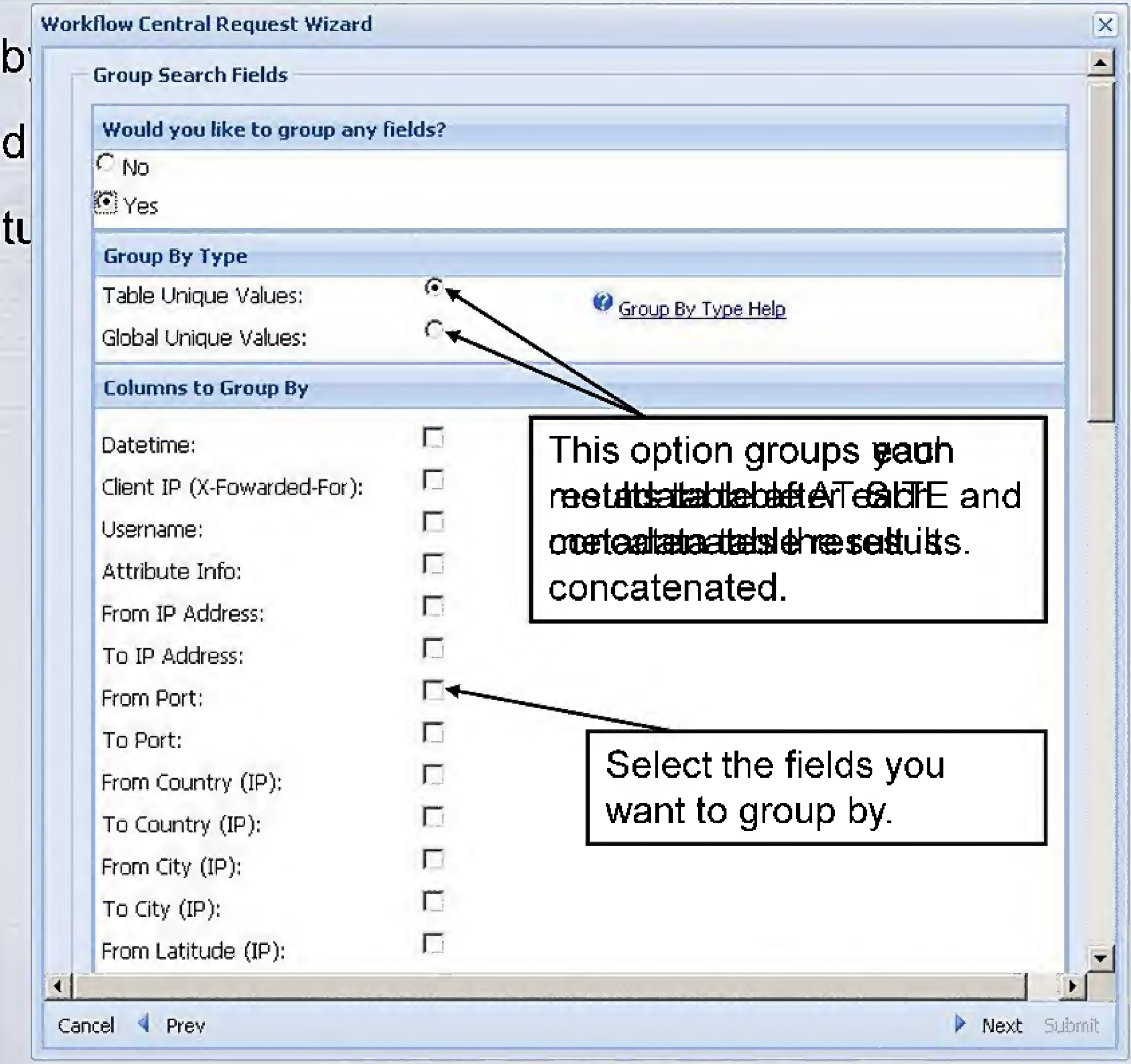
See Search Value Help below for more details or
for a description of boolean logic go to here.

Search Field	Search Value	Remove
From IP Address OR To IP Address	1.2.3.4	✖

or every field, ou must select e PLUS key

Group by option

- Group b ta results.
  - Red
  - Retu



Would you like to group any fields?

○ No
● Yes

Group By Type

Table Unique Values: ●
Global Unique Values: ○

Columns to Group By

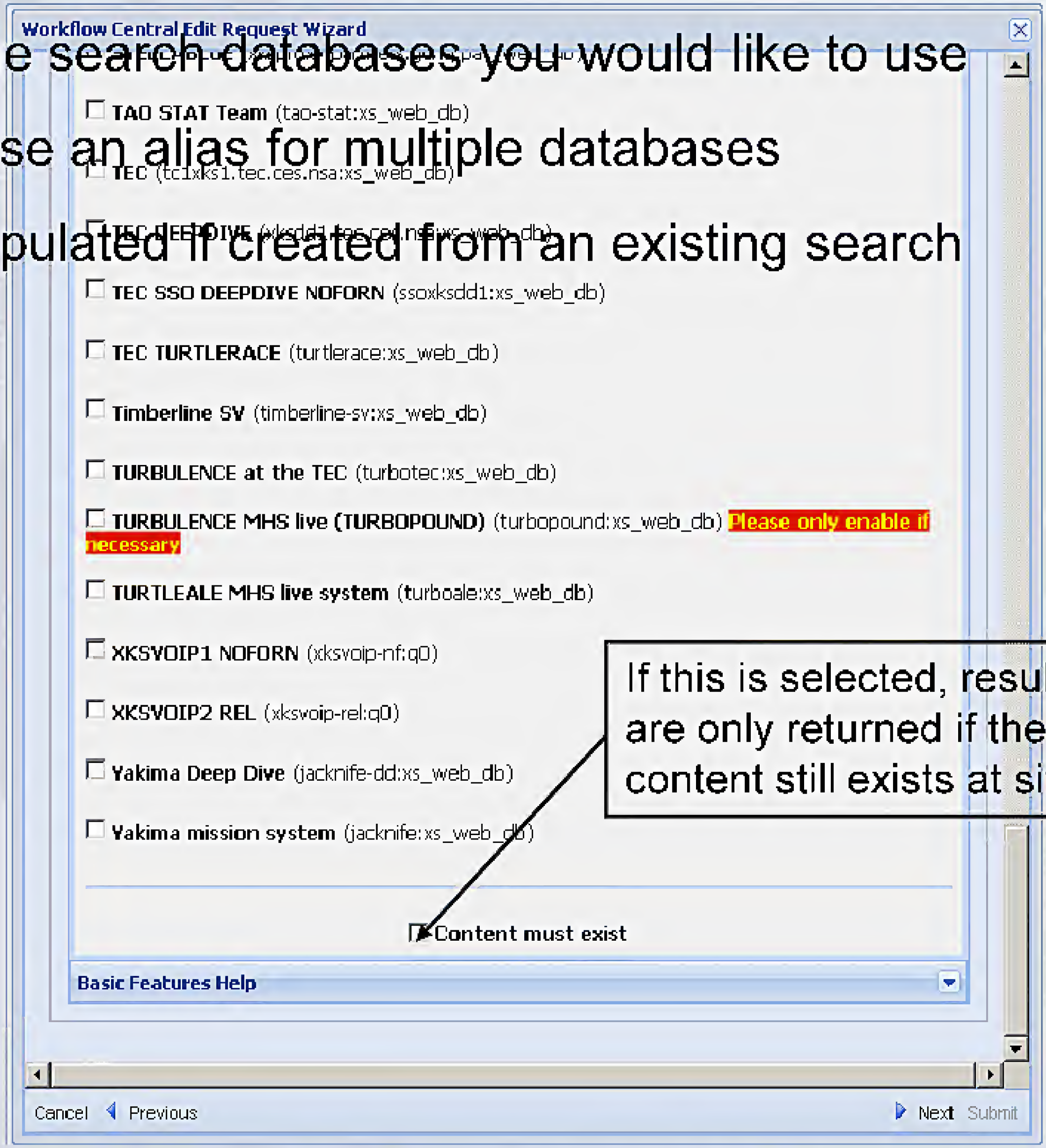
- Datetime: □
- Client IP (X-Fowarded-For): □
- Username: □
- Attribute Info: □
- From IP Address: □
- To IP Address: □
- From Port: □
- To Port: □
- From Country (IP): □
- To Country (IP): □
- From City (IP): □
- To City (IP): □
- From Latitude (IP): □

This option groups each result table after SITE and concatenates the results. concatenated.

Select the fields you want to group by.

Select databases

- Choose the search databases you would like to use
  - Can use an alias for multiple databases
  - Prepopulated if created from an existing search



☐ **TAO STAT Team** (tao-stat:xs_web_db)

☐ **TEC** (tc1xks1.tec.ces.nsa:xs_web_db)

☐ **TEC DEEPDIVE** (xksdd1.tec.ces.nsa:xs_web_db)

☐ **TEC SSO DEEPDIVE NOFORN** (ssoxksdd1:xs_web_db)

☐ **TEC TURTLERACE** (turtlerace:xs_web_db)

☐ **Timberline SV** (timberline-sv:xs_web_db)

☐ **TURBULENCE at the TEC** (turbotec:xs_web_db)

☐ **TURBULENCE MHS live (TURBOPOUND)** (turbopound:xs_web_db) **Please only enable if necessary**

☐ **TURTLEALE MHS live system** (turboale:xs_web_db)

☐ **XKSVOIP1 NOFORN** (xksvoip-nf:q0)

☐ **XKSVOIP2 REL** (xksvoip-rel:q0)

☐ **Yakima Deep Dive** (jacknife-dd:xs_web_db)

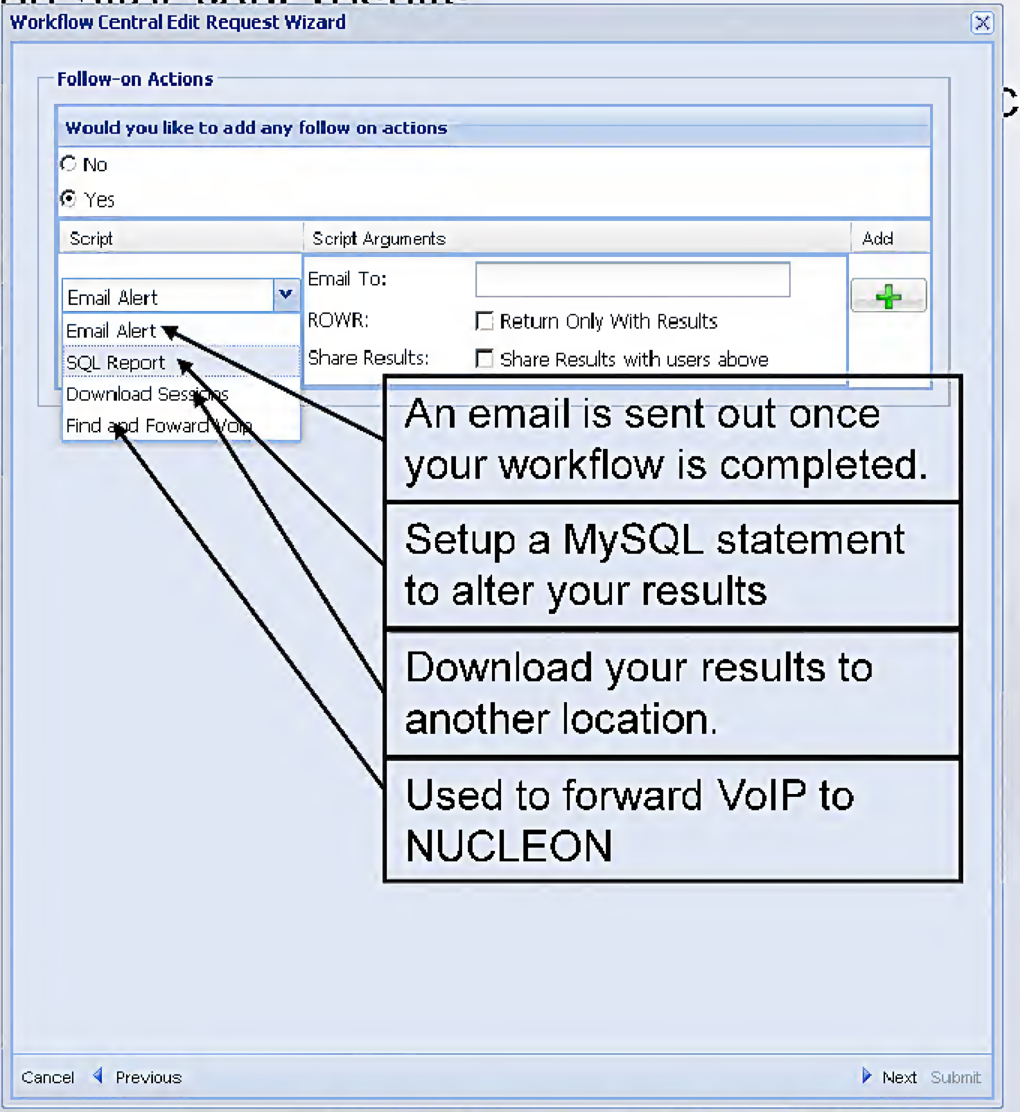
☐ **Yakima mission system** (jacknife:xs_web_db)

☐ Content must exist

If this is selected, results are only returned if the content still exists at site.

Follow on Actions

- Allows you alter your results
- Allows y content) to another location.
- Allows y
- Allows y



Workflow Central Edit Request Wizard

Follow-on Actions

Would you like to add any follow on actions

○ No

● Yes

Script	Script Arguments		Add
Email Alert	Email To:		+
	ROWR:	□ Return Only With Results	
	Share Results:	□ Share Results with users above	

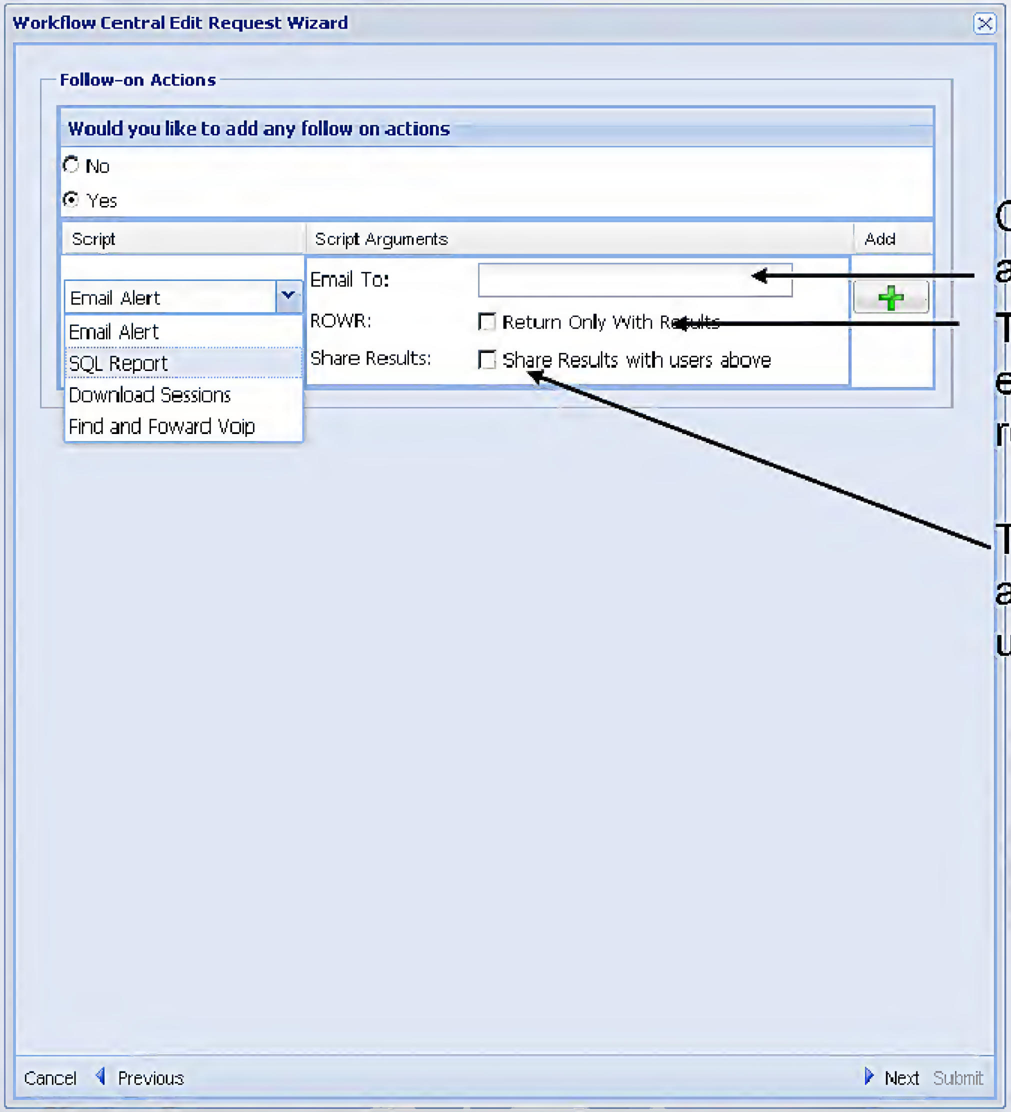
An email is sent out once your workflow is completed.

Setup a MySQL statement to alter your results

Download your results to another location.

Used to forward VoIP to NUCLEON

Email alert



Workflow Central Edit Request Wizard

Follow-on Actions

Would you like to add any follow on actions

○ No

● Yes

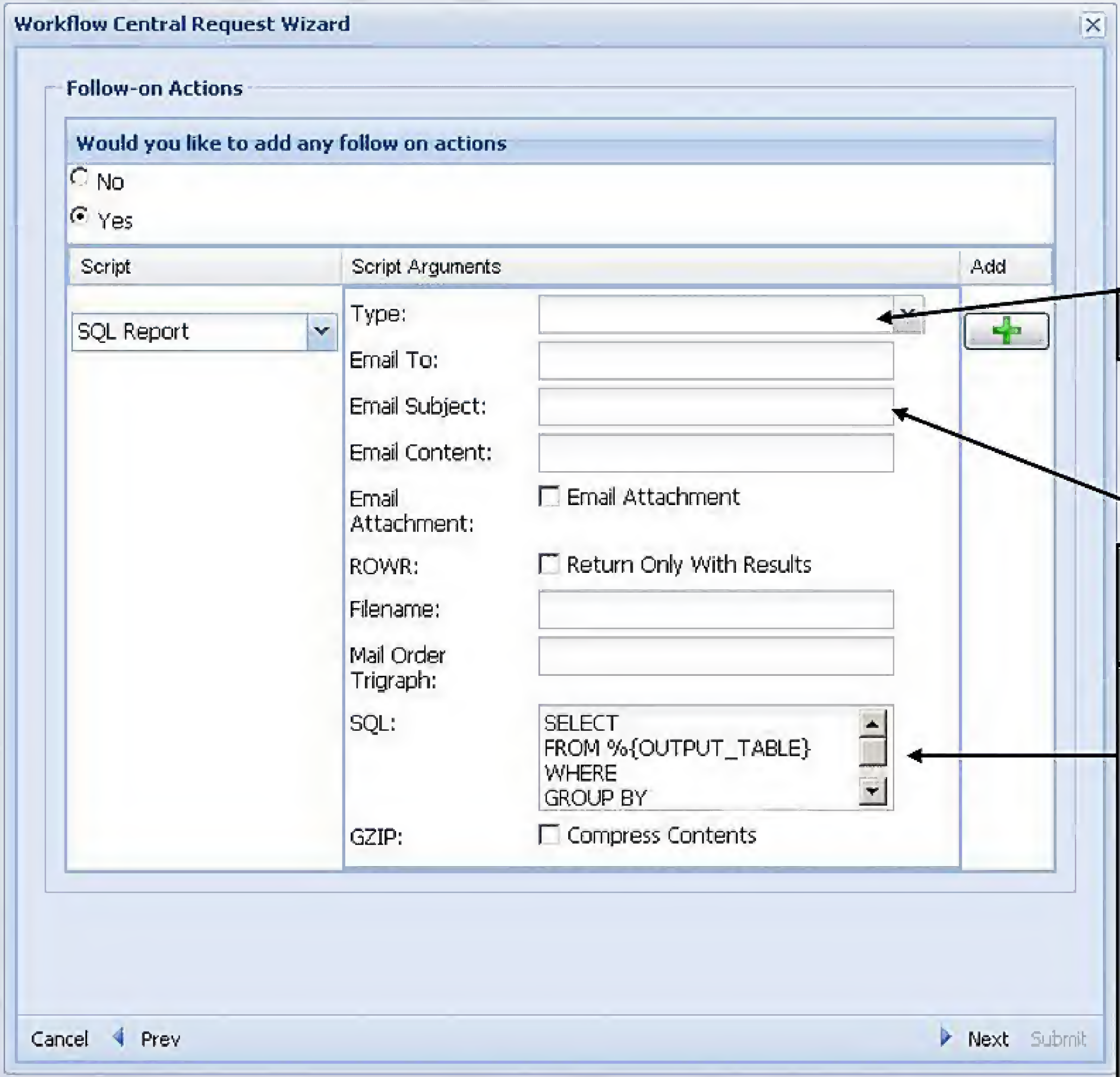
Script	Script Arguments		Add
Email Alert	Email To:		+
	ROWR:	□ Return Only With Results	
	Share Results:	□ Share Results with users above	

Comma delimited email addresses.

This option only sends an email if you workflow has results.

This will make the results appear for all of the listed users

SQL report



Workflow Central Request Wizard

Follow-on Actions

Would you like to add any follow on actions

○ No

● Yes

Script	Script Arguments		Add
SQL Report	Type:		+
	Email To:		
	Email Subject:		
	Email Content:		
	Email Attachment:	□ Email Attachment	
	ROWR:	□ Return Only With Results	
	Filename:		
	Mail Order Trigraph:		

	SQL:	SELECT
		FROM %{OUTPUT_TABLE}
		WHERE
		GROUP BY	

	GZIP:	□ Compress Contents	

CSV or HTML

Email metadata that a user can set.

This must be a VALID SQL statement.

Example:

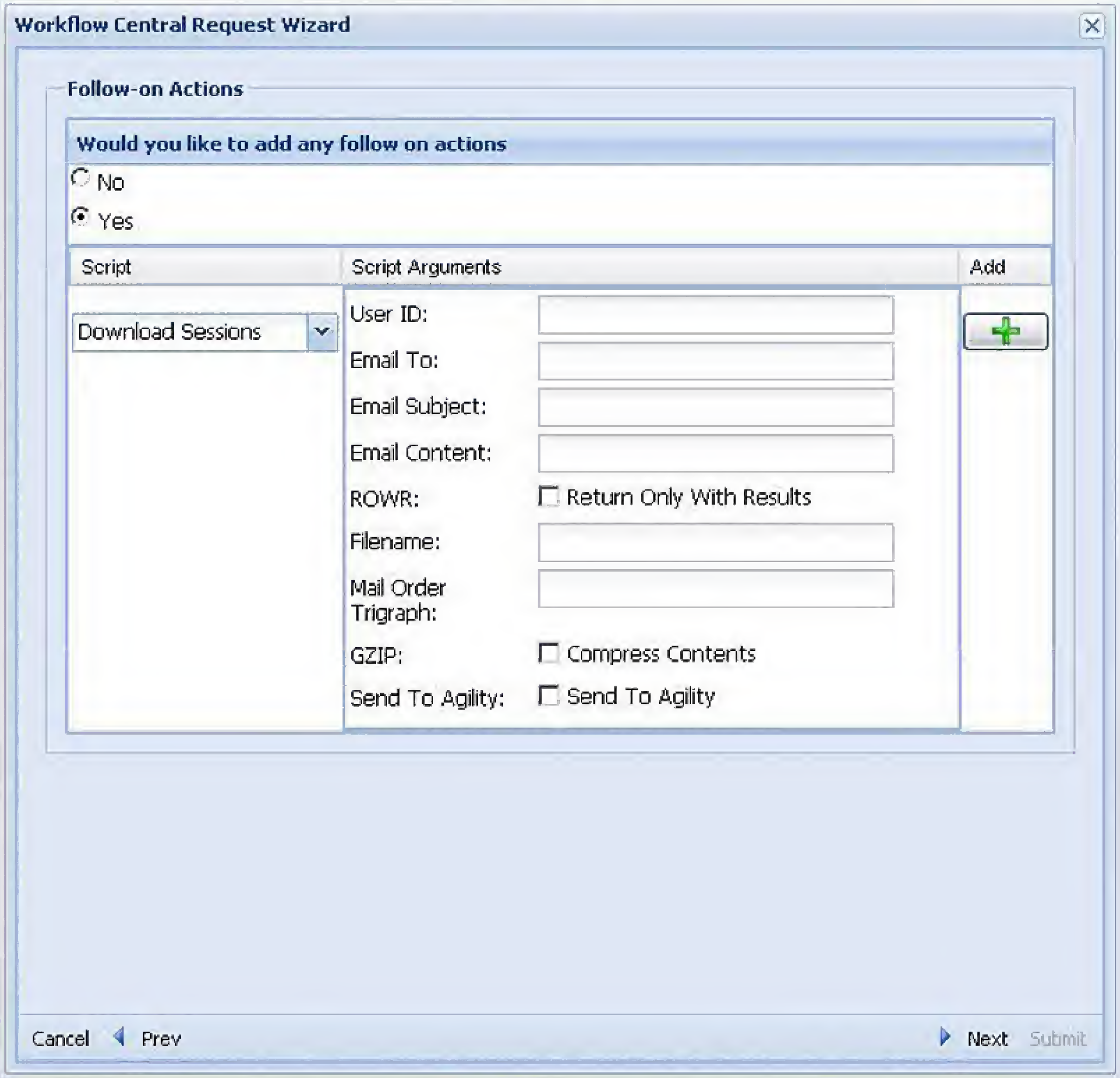
SELECT casenotation, sigad

FROM %{OUTPUT_TABLE}

WHERE sigad!=''

GROUP BY casenotation

Download Results



Workflow Central Request Wizard

Follow-on Actions

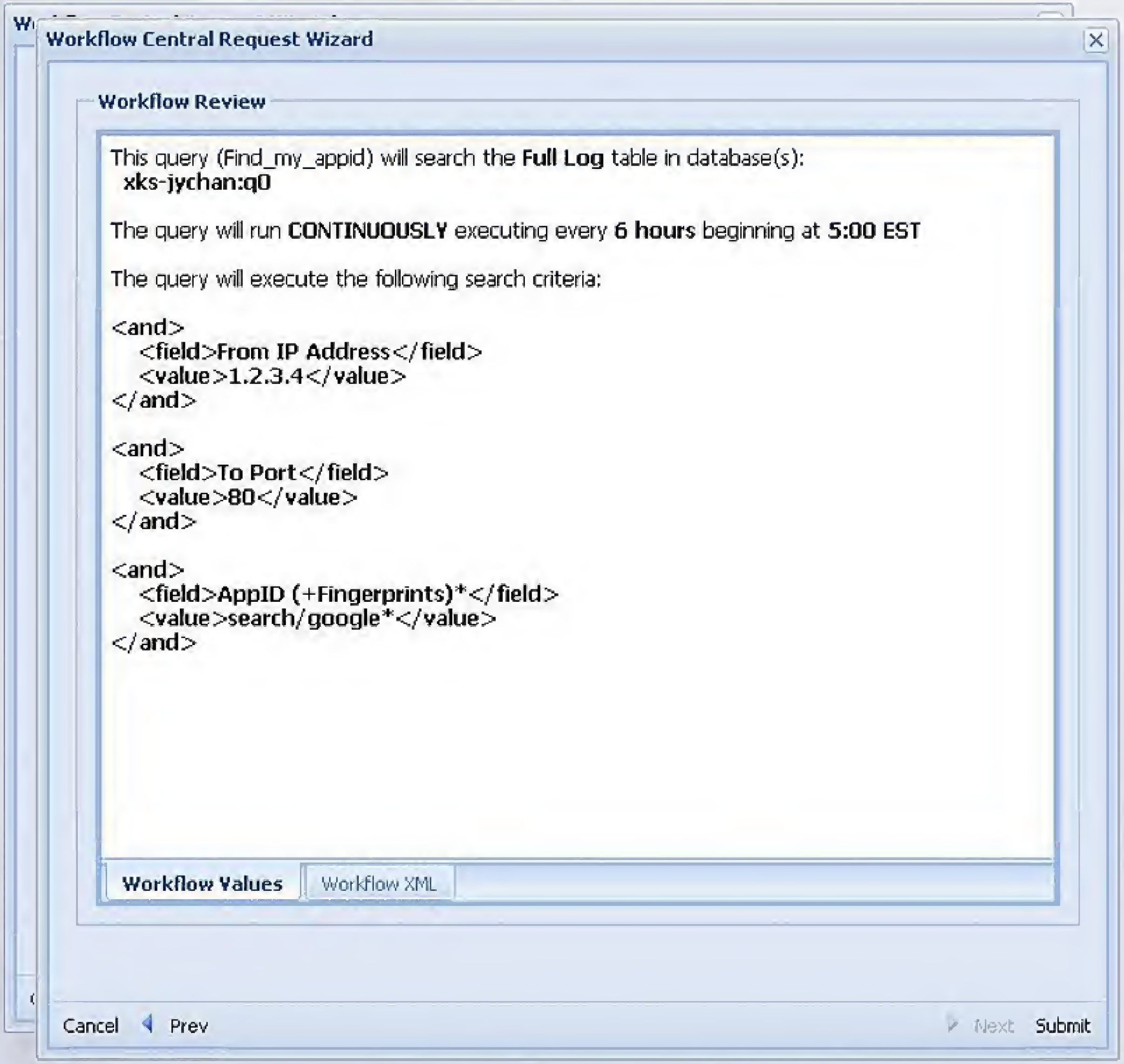
Would you like to add any follow on actions

○ No

● Yes

Script	Script Arguments		Add
Download Sessions	User ID:		+
	Email To:		
	Email Subject:		
	Email Content:		
	ROWR:	□ Return Only With Results	
	Filename:		
	Mail Order Trigraph:		
	GZIP:	□ Compress Contents	
	Send To Agility:	□ Send To Agility	

You're almost done!



This query (Find_my_appid) will search the **Full Log** table in database(s):
xks-jychan:q0

The query will run **CONTINUOUSLY** executing every **6 hours** beginning at **5:00 EST**

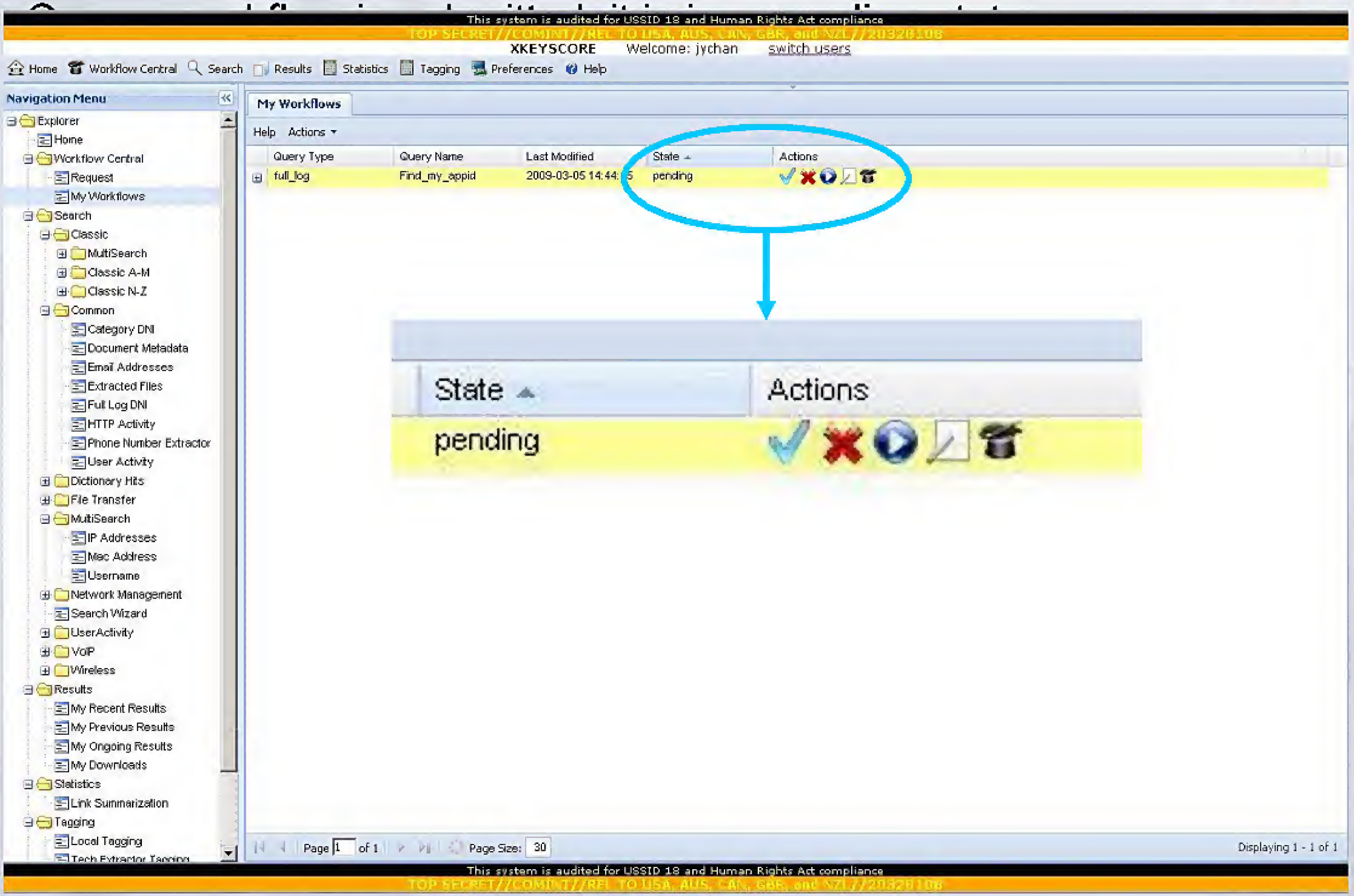
The query will execute the following search criteria:

```
<and>
   <field>From IP Address</field>
   <value>1.2.3.4</value>
</and>

<and>
   <field>To Port</field>
   <value>80</value>
</and>

<and>
   <field>AppID (+Fingerprints)*</field>
   <value>search/google*</value>
</and>
```

Workflow Pending



This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

XKEYSCORE Welcome: jychan switch users

Query Type	Query Name	Last Modified	State	Actions
full_log	Find_my_appid	2009-03-05 14:44:5	pending	✓ ✗

State

Actions

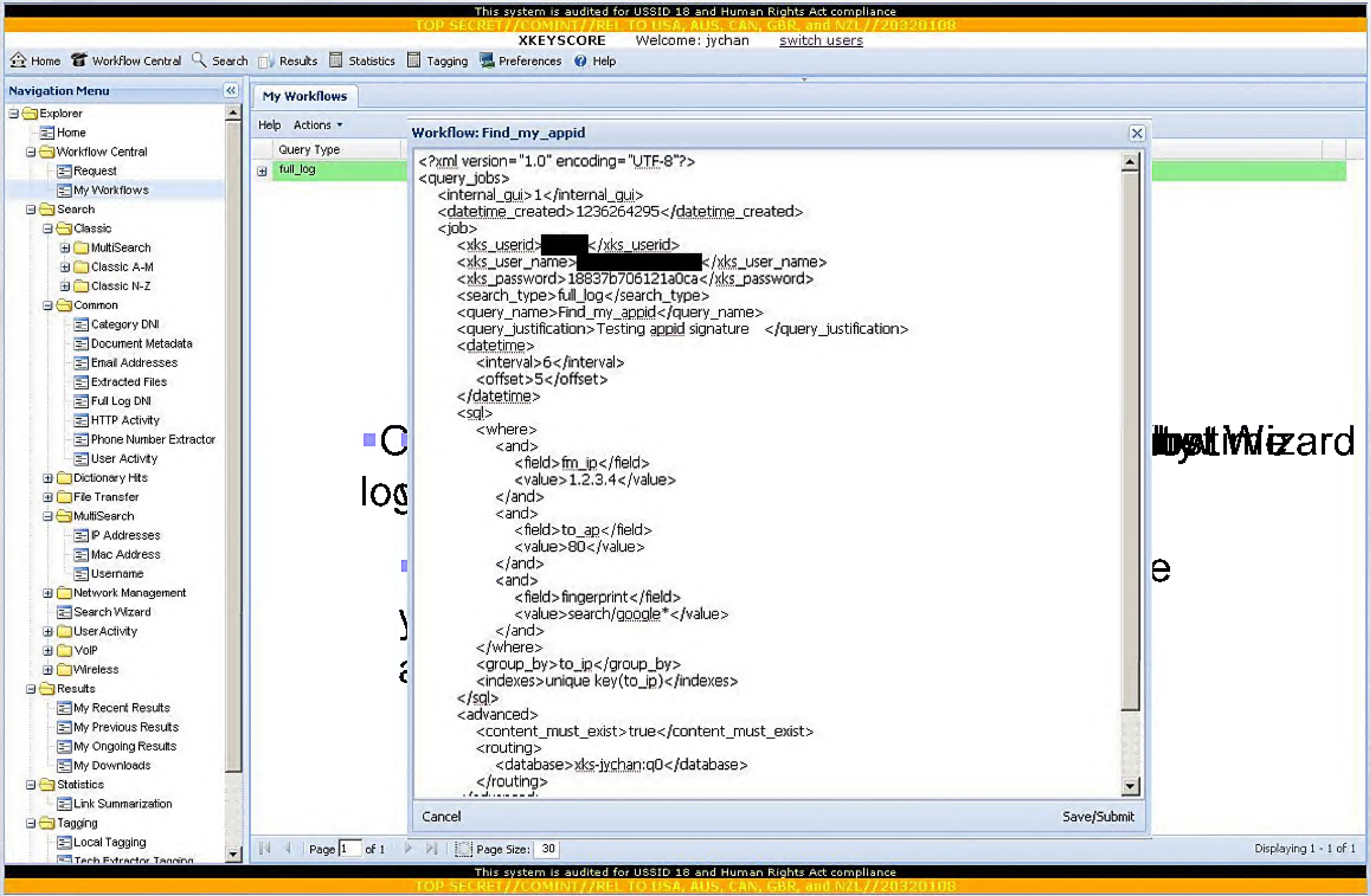
pending

Page 1 of 1 Page Size: 30 Displaying 1 - 1 of 1

This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

Workflow Approved



This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

XKEYSCORE Welcome: jychan switch users

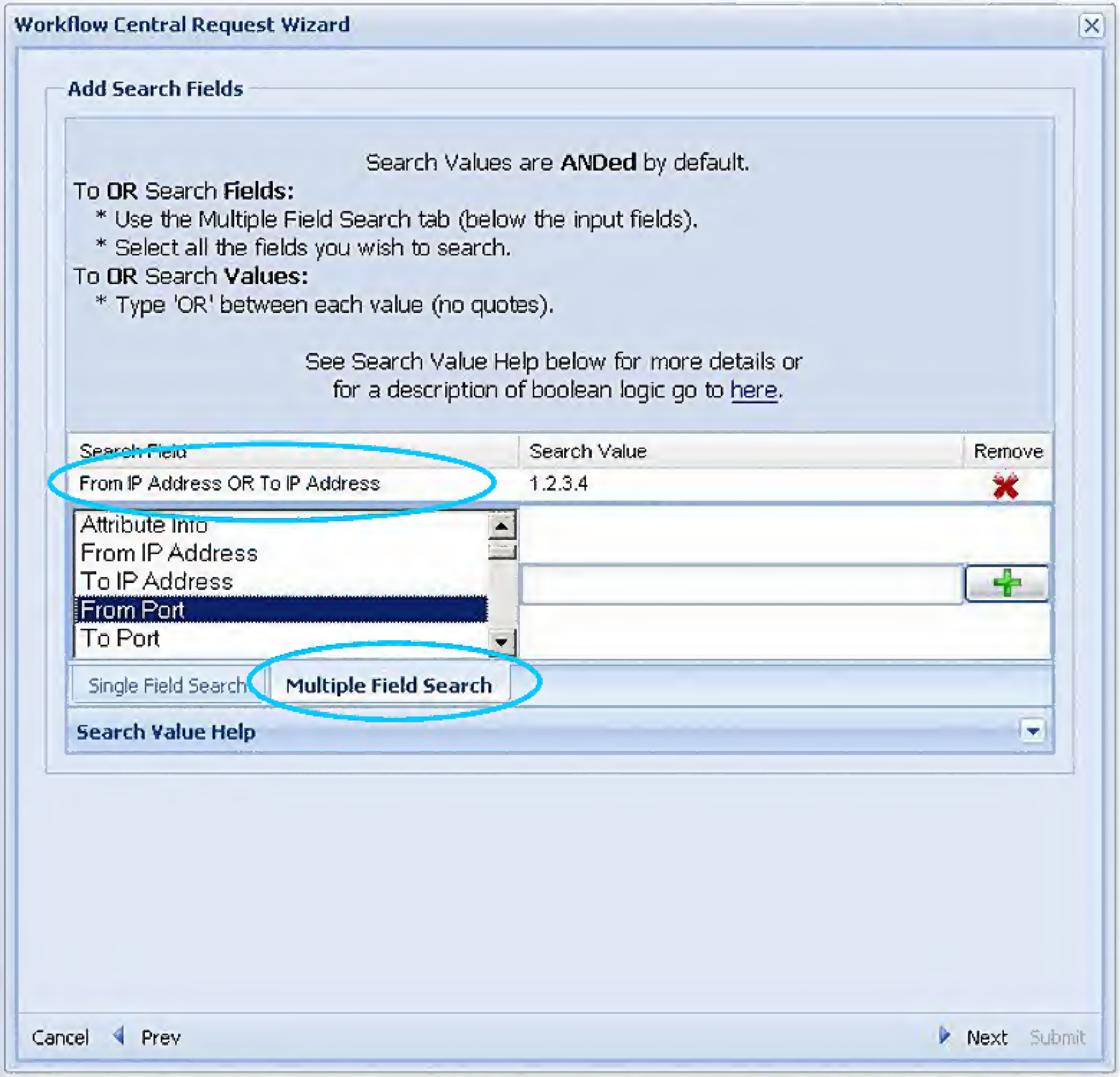
```
<?xml version="1.0" encoding="UTF-8"?>
<query_jobs>
  <internal_gui>1</internal_gui>
  <datetime_created>1236264295</datetime_created>
  <job>
    <xks_userid>[redacted]</xks_userid>
    <xks_user_name>[redacted]</xks_user_name>
    <xks_password>18837b706121a0ca</xks_password>
    <search_type>full_log</search_type>
    <query_name>Find_my_appid</query_name>
    <query_justification>Testing appid signature    </query_justification>
    <datetime>
      <interval>6</interval>
      <offset>5</offset>
    </datetime>
    <sql>
      <where>
        <and>
          <field>fm_ip</field>
          <value>1.2.3.4</value>
        </and>
        <and>
          <field>to_ap</field>
          <value>80</value>
        </and>
        <and>
          <field>fingerprint</field>
          <value>search/google*</value>
        </and>
      </where>
      <group_by>to_ip</group_by>
      <indexes>unique key(to_ip)</indexes>
    </sql>
    <advanced>
      <content_must_exist>true</content_must_exist>
      <routing>
        <database>xks-jychan:q0</database>
      </routing>
```

This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

Common mistakes

- From IP and To IP with the same value.
- In this view, terms are ANDed together.
- Use Multiple Field Search Tab.



Workflow Central Request Wizard

Add Search Fields

Search Values are **AND**ed by default.

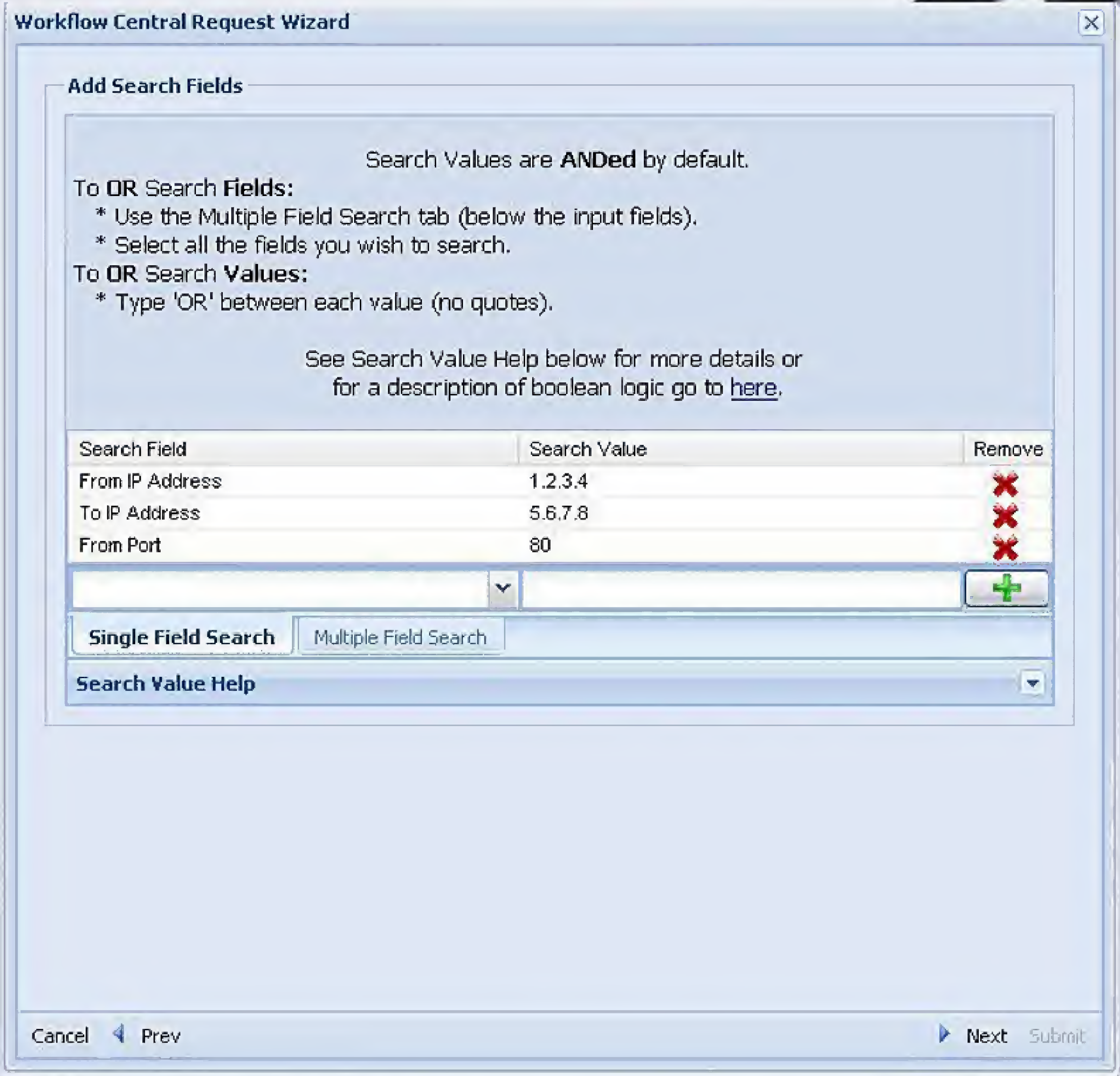
To **OR** Search **Fields:**
* Use the Multiple Field Search tab (below the input fields).
* Select all the fields you wish to search.
To **OR** Search **Values:**
* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or
for a description of boolean logic go to here.

Search Field	Search Value	Remove
From IP Address OR To IP Address	1.2.3.4	✖

Common mistakes

- Using the multiple field search does not break this up into 3 search<->value pairs.
- Enter each term separately in the single fieldsearch.



Workflow Central Request Wizard

Add Search Fields

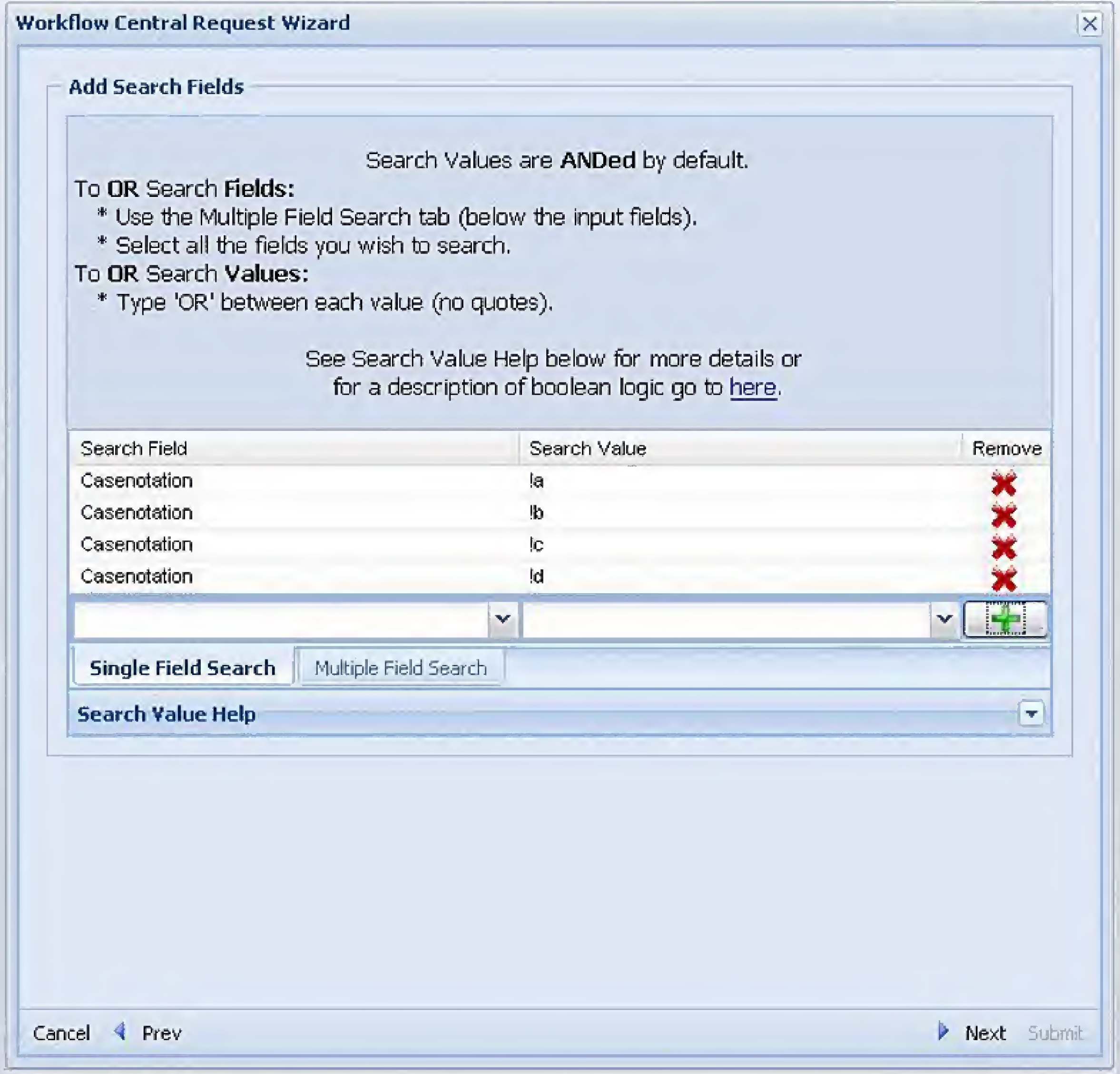
Search Values are **ANDed** by default.
To **OR** Search **Fields:**
* Use the Multiple Field Search tab (below the input fields).
* Select all the fields you wish to search.
To **OR** Search **Values:**
* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or
for a description of boolean logic go to here.

Search Field	Search Value	Remove
From IP Address	1.2.3.4	✗
To IP Address	5.6.7.8	✗
From Port	80	✗

Common mistakes

- This will return ALL casenotations.
  - a will be deafeted by “!a” but a does equal “!b”
- All the defeated values must be ANDed together.



Workflow Central Request Wizard

Add Search Fields

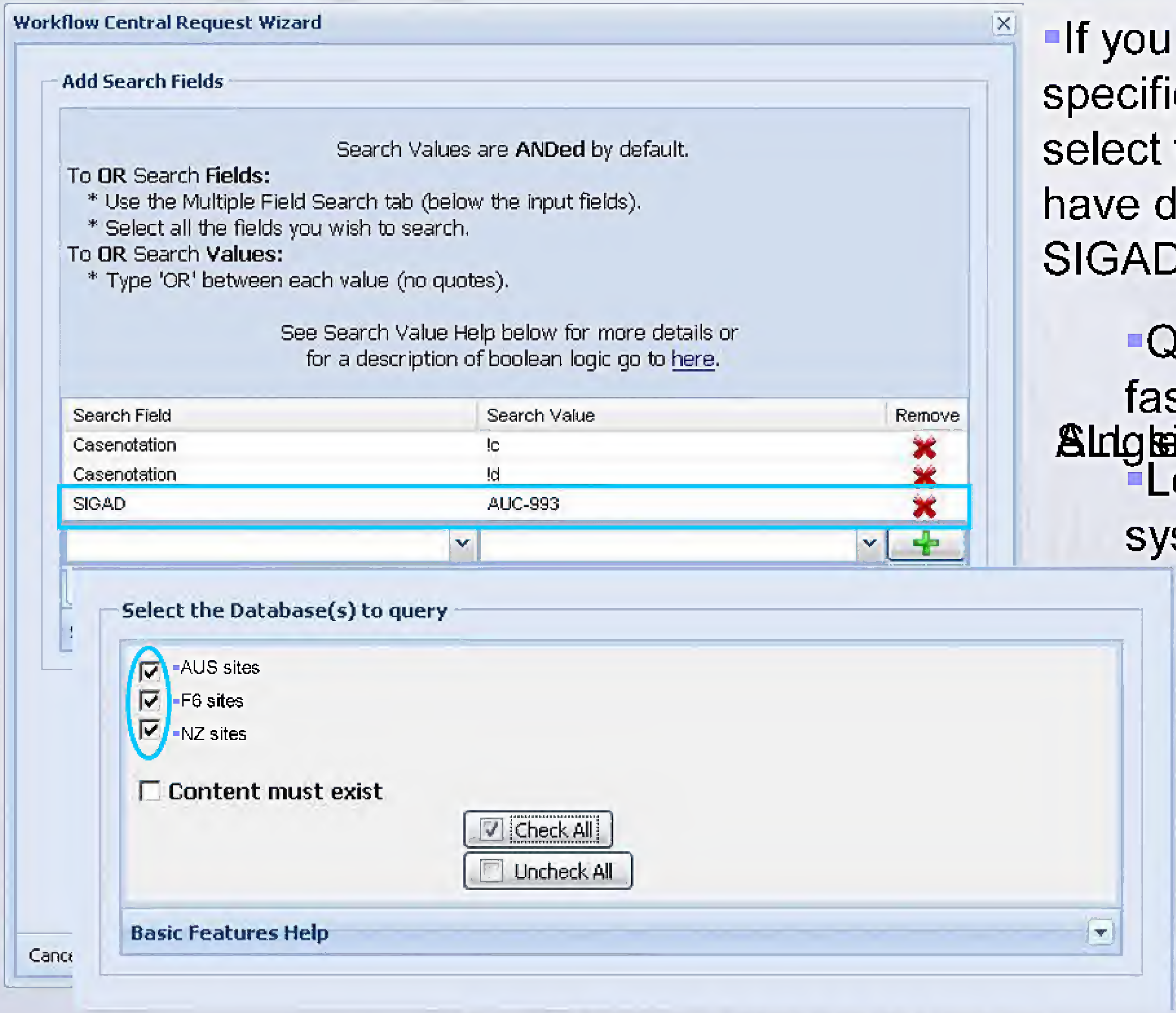
Search Values are **ANDed** by default.

To **OR** Search **Fields:**
* Use the Multiple Field Search tab (below the input fields).
* Select all the fields you wish to search.
To **OR** Search **Values:**
* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or
for a description of boolean logic go to here.

Search Field	Search Value	Remove
Casenotation	!a	✖
Casenotation	!b	✖
Casenotation	!c	✖
Casenotation	!d	✖

Common mistakes



Workflow Central Request Wizard

Add Search Fields

Search Values are **ANDed** by default.

To **OR** Search **Fields:**
- * Use the Multiple Field Search tab (below the input fields).
- * Select all the fields you wish to search.

To **OR** Search **Values:**
- * Type 'OR' between each value (no quotes).

See Search Value Help below for more details or for a description of boolean logic go to here.

Search Field	Search Value	Remove
Casenotation	!c	✖
Casenotation	!d	✖
SIGAD	AUC-993	✖

Select the Database(s) to query

- ☑ AUS sites
- ☑ F6 sites
- ☑ NZ sites

□ **Content must exist**

- If you are selecting specific SIGADs, only select the sites that have data from that SIGAD.
  - Queries will return faster.

All sites selected

Single SIGAD

  - Less work for the system.

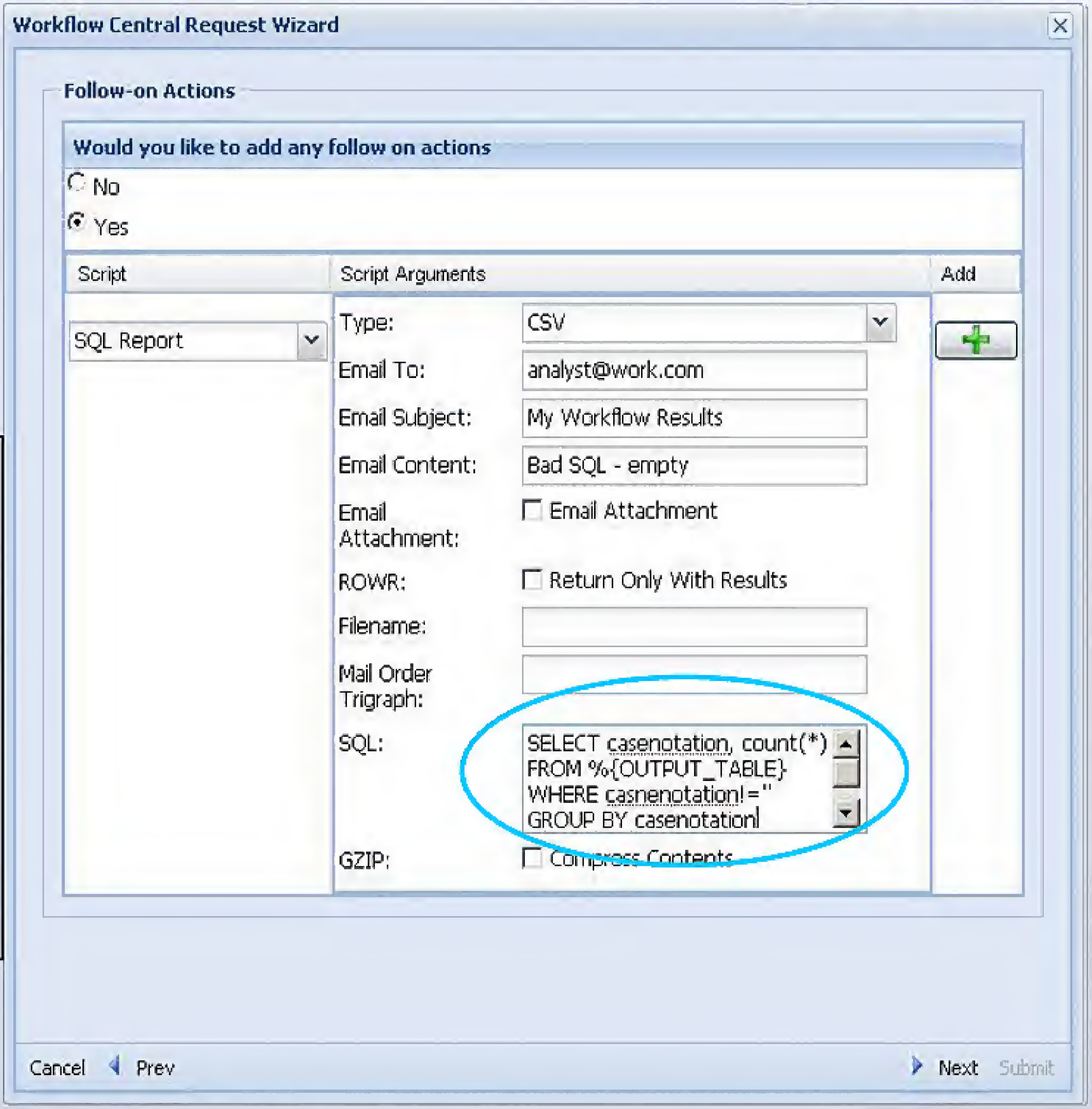
Common mistakes

- If you select the SQL Report option, make sure you put a valid SQL statement!

SQL statement filled in:

SELECT casenotation,
count(*)
FROM %{OUTPUT_TABLE}
WHERE casenotation!=''
GROUP BY casenotation

EMPTY
statement



Workflow Central Request Wizard

Follow-on Actions

Would you like to add any follow on actions

○ No
● Yes

Script	Script Arguments		Add
SQL Report	Type:	CSV	+
	Email To:	analyst@work.com	
	Email Subject:	My Workflow Results	
	Email Content:	Bad SQL - empty	
	Email Attachment:	□ Email Attachment	
	ROWR:	□ Return Only With Results	
	Filename:		
	Mail Order Trigraph:		

	SQL:	SELECT casenotation, count(*)
		FROM %{OUTPUT_TABLE}
		WHERE casnenotation!=''
		GROUP BY casenotation	

	GZIP:	□ Compress Contents	

XKEYSCORE

Questions?

xks_workflow@r1.r.nsa